cycura

Kontrolle über privilegierte Zugriffe

cycura.de

Ihre Admin-Identitäten haben keinen Schutzraum

Sie haben E5-Lizenzen, PIM und Conditional Access implementiert. Ihre Sicherheitsstrategie sieht gut aus auf dem Papier. In der Praxis greifen Ihre Administratoren aber vom selben Laptop auf kritische Systeme zu, mit dem sie eben noch E-Mails geöffnet haben. Die Trennung zwischen normalem Betrieb und privilegierten Zugriffen existiert nicht strukturell – und genau dort liegt das Problem.

Was Sie in diesem Guide erwarten

- Die 4 kritischen Lücken in Ihrer Admin-Architektur
- Warum Identitäts-Sicherheit allein nicht ausreicht
- Das Managed-Red-Tenant-Modell für strukturelle Isolation
- Ein 12-Punkte-Check zur Bewertung Ihres aktuellen Risikos

80%

bis zu 80% der Unternehmen haben keine isolierte Admin-Infrastruktur

67%

rund zwei Drittel nutzen Standard-Endgeräte für administrative Zugriffe

90%

über 90% erfolgreicher Lateral-Movement-Angriffe involvieren privilegierte Identitäten

Vier Lücken, die Ihre Admin-Sicherheit untergraben

1 **Admin-Zugriffe vom Standard-Arbeitsplatz**

Ihre Administratoren nutzen denselben Laptop für E-Mails und privilegierte Systemzugriffe. Ein kompromittiertes Endgerät öffnet direkt den Weg in Ihre kritische Infrastruktur.

2 **Die Hälfte Ihrer privilegierten Konten ist unbekannt**

Sie dokumentieren zehn Global-Admins, tatsächlich existieren vierzig. Unüberwachte Accounts mit weitreichenden Rechten bleiben unter dem Radar.

3 **Keine Trennung zwischen User- und Admin-Identitäten**

Dieselben Anmeldedaten dienen dem Mail-Verkehr und dem Zugriff auf Domain-Controller. Ein erfolgreicher Phishing-Angriff reicht für vollständige Systemkontrolle.

4 **Notfallzugriffe ohne Kontrolle**

Break-Glass-Passwörter liegen im internen Wiki, zugänglich für das gesamte IT-Team. Eine Nutzungsprotokollierung existiert nicht.

Strukturelle Trennung fehlt

Die meisten Unternehmen haben ihre Sicherheitsmaßnahmen auf der Identitätsebene optimiert. PIM, MFA, Conditional Access – alles vorhanden. Doch die Architektur, also die strukturelle Trennung zwischen Admin- und Normalbetrieb, wurde nicht angefasst. Das Resultat: drei kritische Lücken, die Ihre gesamte Sicherheitsinvestition untergraben.

1

Keine Isolation

Administrative Zugriffe laufen über dieselben Endpunkte, dieselben Netzwerke, dieselben Identitäten wie der normale Betrieb. Ein kompromittierter Admin-Laptop bedeutet: Der Angreifer ist bereits in Ihrem Netzwerk – mit vollen Rechten. Es gibt keine technische Barriere, die ihn aufhält.

2

Keine Kontrolle

Sie wissen nicht lückenlos, wer wann von welchem Endpunkt aus administrative Tätigkeiten ausführt. Bei einem Sicherheitsvorfall fehlt Ihnen die Transparenz, um schnell zu reagieren. Die Nachvollziehbarkeit ist nicht gegeben.

3

Keine Resilienz

Die Kompromittierung eines einzelnen Admin-Accounts gefährdet Ihre gesamte Umgebung. Es gibt keine Blast-Radius-Reduktion. Ein Phishing-Klick, eine Malware-Infektion – und der Angreifer hat Zugang zu Ihrem gesamten Unternehmen.

Das Business-Risiko

Ein kompromittierter Admin-Account ermöglicht Angreifern typischerweise den schnellsten Weg durch Ihre Umgebung. Die durchschnittliche Zeit zwischen erstem Zugriff und vollständiger Domain-Übernahme liegt bei **24–48 Stunden** (Mandiant, 2023). Die Kosten eines Ransomware-Angriffs belaufen sich im Mittel auf **4,45 Millionen US-Dollar** (IBM, 2023) – zuzüglich regulatorischer Konsequenzen und Reputationsverlust.

Die 5 kritischen Architekturlücken

1 Admin-Zugriffe vom Produktiv-Endpoint

Kritikalität: Hoch Häufigkeit: 85%

DIE LÜCKE

Administrative Zugriffe auf Azure AD, Microsoft 365 und Cloud-Ressourcen erfolgen über dieselben Endpunkte, die für E-Mail und Web-Browsing genutzt werden. Dedizierte Admin-Workstations existieren nicht oder werden nicht konsequent eingesetzt.

DAS KONKRETE RISIKO

Schadsoftware auf dem Admin-Laptop – durch Phishing, kompromittierte Downloads oder Supply-Chain-Angriffe – hat direkten Zugriff auf aktive Admin-Sessions. Ein Keylogger oder Credential-Dumper genügt, um administrative Berechtigungen zu erlangen. Der Angreifer sitzt auf demselben Gerät wie Ihr Admin – mit denselben Rechten.

WAS WIR IN DER PRAXIS FINDEN

Admins, die vom normalen Arbeitslaptop aus Global-Admin-Aufgaben erledigen – parallel zum Surfen im Internet. Die Migration auf dedizierte Workstations wurde nicht abgeschlossen. Die Policy existiert, die Governance für konsequente Durchsetzung fehlt.

UNSER ANSATZ

Strikte Trennung durch dedizierte Admin-Workstations (PAWs) mit gehärtetem Betriebssystem, isoliertem Netzwerk und keinem Internetzugriff. Alternative: Virtual Admin Workstations (VAWs) über Azure Virtual Desktop.

Die 5 kritischen Architekturlücken

2 Gemeinsame Identitäten für User und Admin

Kritikalität: Kritisch Häufigkeit: 70%

DIE LÜCKE

Dieselbe Identität wird für reguläre Benutzeraktivitäten (E-Mail, Teams) und administrative Aufgaben verwendet. Die Identität verfügt über dauerhaft erhöhte Rechte oder kann diese selbstständig aktivieren.

DAS KONKRETE RISIKO

Ein erfolgreicher Phishing-Angriff auf einen User-Account mit administrativen Rechten führt direkt zur Kompromittierung privilegierter Zugriffe. Der Angreifer benötigt kein spezifisches Wissen über Ihre Admin-Systeme – die Standard-Anmeldedaten Ihres Mitarbeiters genügen. Das E-Mail-Postfach Ihres CIOs ist gleichzeitig Ihr höchstes Sicherheitsrisiko.

WAS WIR IN DER PRAXIS FINDEN

Der CIO nutzt seine normale E-Mail-Adresse für alle administrativen Aufgaben. Das Konto hat Global-Admin-Rechte und ist in PIM hinterlegt – aber die Aktivierung erfolgt automatisch, ohne zusätzliche Absicherung oder Genehmigung.

UNSER ANSATZ

Vollständige Trennung der Identitäten: Red Accounts im isolierten Tenant für alle Admin-Aktivitäten. User-Accounts haben niemals administrative Rechte. Jede Rechteerweiterung erfordert eine explizite, überwachte Genehmigung.

Die 5 kritischen Architekturlücken

3 Fehlende Netzwerk-Isolation

Kritikalität: Hoch Häufigkeit: 90%

DIE LÜCKE

Admin-Workstations haben uneingeschränkten Internetzugriff und befinden sich im selben Netzwerksegment wie Standard-Benutzer. Netzwerksegmentierung, dedizierte Admin-VLANs und Kontrolle ausgehender Verbindungen fehlen.

DAS KONKRETE RISIKO

Während einer aktiven Admin-Session wird parallel im Internet gesurft, auf Phishing-Links geklickt oder kompromittierte Websites aufgerufen. Ein Angreifer kann über den Browser oder Malware Daten aus der Admin-Session extrahieren. Ihr Admin surft mit vollen Rechten im Internet – ohne technische Barriere, die das verhindert.

WAS WIR IN DER PRAXIS FINDEN

Admins nutzen privilegierte Sessions parallel zur normalen Internet-Nutzung. Keine technische Barriere verhindert, dass während einer Azure-AD-Verwaltung gleichzeitig E-Mails geöffnet oder Websites besucht werden.

UNSER ANSATZ

Strikte Netzwerk-Isolation durch dedizierte Admin-Netzwerke ohne Internetzugriff. Einsatz von Microsoft Global Secure Access für kontrollierten, überwachten Zugriff.

Die 5 kritischen Architekturlücken

4 Unkontrollierte Notfallzugriffe

Kritikalität: Mittel-Hoch **Häufigkeit: 95%**

DIE LÜCKE

Break-Glass-Accounts sind vorhanden, aber unzureichend geschützt. Passwörter werden in Wikis oder SharePoints dokumentiert, MFA fehlt, und die Nutzung wird nicht protokolliert. Mehrere Personen im IT-Team kennen die Zugangsdaten.

DAS KONKRETE RISIKO

Ehemalige Mitarbeiter oder kompromittierte Accounts im IT-Team können Break-Glass-Credentials nutzen, um vollständige Kontrolle zu erlangen – ohne dass die Nutzung protokolliert oder alarmiert wird. Ihre letzte Verteidigungslinie ist öffentlich zugänglich.

WAS WIR IN DER PRAXIS FINDEN

Break-Glass-Account-Passwörter in einem Confluence-Wiki, erreichbar für das gesamte IT-Team. Keine MFA, keine Aktivitätsüberwachung, keine regelmäßigen Passwortwechsel.

UNSER ANSATZ

Break-Glass-Accounts im isolierten Red Tenant mit physisch gesicherten Credentials (Hardware-Token, Safe). Jede Nutzung löst sofortige Alerts aus und erfordert eine Nachbereitung.

Die 5 kritischen Architekturlücken

5 Fehlende Session-Isolierung

Kritikalität: Hoch Häufigkeit: 80%

DIE LÜCKE

Admin-Sessions bleiben über Tage oder Wochen aktiv. Maximale Session-Dauer, erzwungene Re-Authentifizierung und Idle-Timeout fehlen. Administratoren bleiben dauerhaft angemeldet.

DAS KONKRETE RISIKO

Eine kompromittierte, aber noch aktive Admin-Session kann über Wochen für laterale Bewegungen genutzt werden. Der Angreifer muss sich nicht erneut authentifizieren und kann unter Umständen unentdeckt agieren. Ein einmal erbeuteter Zugriff bleibt wochenlang gültig.

WAS WIR IN DER PRAXIS FINDEN

Azure-AD-Portale, die über Wochen geöffnet bleiben. Admin-Sessions ohne Timeout, ohne Re-Authentifizierung, ohne Überwachung.

UNSER ANSATZ

Strikte Session-Management-Richtlinien: Maximale Session-Dauer von 4 Stunden, erzwungene Re-Authentifizierung, automatische Trennung bei Inaktivität nach 15 Minuten.

Die Lösung: Der Managed Red Tenant

Der Managed Red Tenant ist keine Software, die Sie kaufen und installieren. Es ist eine architektonische Entscheidung: die strukturelle Trennung privilegierter Zugriffe vom Produktivbetrieb. Er implementiert das Prinzip der isolierten Verwaltungsumgebung nach dem Microsoft Enterprise Access Model.

Was den Managed Red Tenant auszeichnet

Isolation: Separater Tenant für alle Admin-Aktivitäten. Keine Überschneidung mit dem Produktivtenant.
Zero Trust: Kein implizites Vertrauen. Jeder Zugriff wird explizit authentifiziert und autorisiert.
Clean Source: Admin-Zugriffe erfolgen ausschließlich von gehärteten, isolierten Workstations.
Transparenz: Jede Admin-Handlung ist nachvollziehbar, auditierbar und wird überwacht.

Vorher vs. Nachher

VOR DEM RED TENANT	NACH DEM RED TENANT
Admin-Zugriffe aus dem Produktivtenant	Isolierter Tenant für alle Admin-Aktivitäten
Gemeinsame Identitäten für User und Admin	Getrennte Red Accounts ohne Überschneidung
Keine Netzwerk-Isolation	Vollständige Netzwerk-Isolation
Unkontrollierte Break-Glass-Accounts	Kontrollierte, überwachte Break-Glass-Prozesse
Langlaufende, unüberwachte Sessions	Strikte Session-Kontrolle (max. 4h)

Das Managed Red Tenant Framework

Die Implementierung eines Managed Red Tenant erfolgt in fünf strukturierten Phasen – von der initialen Analyse bis zum kontinuierlichen Betrieb.

1 **Assessment & Trennungsstrategie**

Analyse bestehender Admin-Prozesse, Inventarisierung privilegierter Konten, Definition der PAW/VAW-Strategie, Erstellung der Migrations-Roadmap.

2 **Red Tenant Provisionierung**

Aufbau der isolierten Umgebung, Konfiguration von Entra ID Governance, Implementierung von Global Secure Access, Einrichtung der Monitoring-Infrastruktur.

3 **Identity Segregation**

Trennung der Identitäten (Red Accounts), Migration administrativer Rechte, Eliminierung von Shadow Admins, Implementierung von Just-in-Time-Access.

4 **Workstation Deployment**

Bereitstellung von PAWs für Tier-0, VAWs (Azure Virtual Desktop) für Tier-1/2, Härtung aller Admin-Workstations, Schulung der Administratoren.

5 **Continuous Operation**

24/7-Überwachung administrativer Aktivitäten, proaktives Alerting bei Anomalien, regelmäßige Access Reviews, kontinuierliche Incident Response, fortlaufende Härtung. Der Betrieb wird durch ein dediziertes SOC-Team sichergestellt.

Was der Managed Red Tenant NICHT ist

Kein Ersatz für PAM

Der Red Tenant ergänzt PIM/PAM durch strukturelle Isolation. Beide Konzepte arbeiten komplementär.

Kein Big-Bang-Projekt

Die Migration erfolgt schrittweise, Admin-Gruppe für Admin-Gruppe. Der laufende Betrieb bleibt gewährleistet.

Keine reine Lizenzfrage

E5-Lizenzen erleichtern die Implementierung, aber die Architektur ist entscheidend. Auch mit E3 ist ein Red Tenant realisierbar.

Was er WIRKLICH ist

- ✓ **Ein Zustand:** Administrativer Zugriff ist physisch und logisch vom Standardbetrieb getrennt
- ✓ **Eine Architektur:** Multi-Tenant-Struktur nach Microsoft Enterprise Access Model
- ✓ **Ein Betriebsmodell:** Kontinuierliche Überwachung und Härtung der Admin-Infrastruktur

Wichtiger Hinweis

Der Managed Red Tenant ist keine Software, die Sie kaufen und installieren. Es ist eine architektonische Entscheidung, die Ihre gesamte Herangehensweise an privilegierte Zugriffe verändert. Die Implementierung erfordert strategische Planung, technische Expertise und kontinuierliches Commitment.

Der Reifegrad-Check: Wo stehen Sie?

Bewerten Sie Ihre aktuelle Privileged Access Maturity anhand von fünf definierten Stufen. Jede Stufe repräsentiert einen anderen Grad an Isolation und Kontrolle.

STUFE	BEZEICHNUNG	BESCHREIBUNG
Stufe 1	Ad-hoc	Admins arbeiten auf Standard-Laptops. Keine Trennung von User- und Admin-Aktivitäten. Keine PAWs, keine Netzwerk-Isolation.
Stufe 2	Definiert	PAWs wurden bereitgestellt, aber die Nutzung ist inkonsistent. Ausnahmeprozesse im Arbeitsalltag untergraben die vollständige Durchsetzung.
Stufe 3	Gesteuert	PIM ist aktiv, aber im selben Tenant. Admin-Identitäten sind teilweise getrennt, jedoch nicht isoliert.
Stufe 4	Optimierend	Red Tenant ist etabliert, PAWs/VAWs werden genutzt. Lücken bei der kontinuierlichen Überwachung bestehen noch.
Stufe 5	Exzellent	Vollständige Isolation, Zero Trust implementiert, automatisierte Response auf Anomalien, kontinuierliche Härtung.

Ihre nächsten Schritte

Stufe 1-2: Sofortige Evaluierung eines Red Tenant. Ihr Risiko ist kritisch.

Stufe 3: Planung der Tenant-Trennung. Sie haben die Grundlagen, fehlt die Isolation.

Stufe 4: Optimierung der Überwachung und Automatisierung der Response.

Stufe 5: Kontinuierliche Verbesserung und Red-Teaming.

Der 12-Punkte Risiko-Check

> Beantworten Sie die folgenden Fragen mit Ja oder Nein. Jedes "Nein" signalisiert ein potenzielles Risiko in Ihrer privilegierten Zugriffsarchitektur.

IDENTITÄT & ZUGRIFF

1. Haben Sie eine vollständige Übersicht über alle privilegierten Identitäten in Ihrer Umgebung?
2. Sind Admin-Zugriffe physisch getrennt vom normalen User-Betrieb (dedizierte Workstations)?
3. Wissen Sie jederzeit, wer Global Admin ist und warum diese Berechtigung besteht?
4. Gibt es eine enforced Clean-Source-Policy für Tier-0-Administratoren?

INFRASTRUKTUR

5. Sind Ihre Admin-Workstations gehärtet und isoliert (kein Internet, eigene VLANs)?
6. Gibt es keinen direkten Internetzugriff von Admin-Workstations?
7. Sind Admin-Sessions zeitlich begrenzt (maximal 4 Stunden)?

RESILIENZ

8. Können Sie einen Notfallzugriff in unter 15 Minuten kontrolliert bereitstellen?
9. Ist laterales Bewegen von einem kompromittierten Admin-Account technisch erschwert?
10. Werden Admin-Aktivitäten in Echtzeit überwacht und bei Anomalien alarmiert?

Der 12-Punkte Risiko-Check

GOVERNANCE

11 Gibt es einen dokumentierten, genehmigten Prozess für neue Admin-Rechte?

12 Können Sie einem Auditor nachweisen, wer wann Zugriff hatte und warum?

Auswertung

"NEIN"-ANTWORTEN	RISIKOSTUFE	EMPFOHLENE MASSNAHME
0-2	Niedriges Risiko	Weiterentwicklung bestehender Maßnahmen
3-5	Mittleres Risiko	Quick Wins identifizieren und umsetzen
6-8	Hohes Risiko	Sofortmaßnahmen erforderlich
9-12	Kritisches Risiko	Red-Tenant-Implementierung priorisieren

Die meisten Unternehmen landen bei **6-8 "Nein"-Antworten** – im Bereich des hohen Risikos. Das ist keine Ausnahme, sondern die typische Ausgangslage. Entscheidend ist das Handeln: Jeder Tag ohne strukturelle Verbesserungen erhöht Ihre Angriffsfläche.

cycura

Der 15-Punkte Risiko-Check

Beantworten Sie die folgenden Fragen mit Ja oder Nein. Jedes "Nein" ist ein potenzielles Risiko.

Kategorie: Identität & Zugriff

- [ ] **1. Transparenz uber alle Identitäten**
  Wissen Sie jederzeit, welche Identitäten (User, Gaste, Apps) aktuell Zugriff auf kritische Ressourcen haben – und warum?
- [ ] **2. Konsistente Absicherung aller Zugriffspfade**
  Sind alle Zugriffspfade (inkl. Azure, APIs, CLI, Service Principals) konsistent abgesichert – ohne blinde Flecken?
- [ ] **3. Begründung privilegierter Berechtigungen**
  Können Sie jede privilegierte Berechtigung fachlich begründen und jederzeit rechtfertigen?
- [ ] **4. Zeitlich begrenzter privilegierter Zugriff**
  Ist privilegierter Zugriff zeitlich begrenzt, nachvollziehbar und aktiv überwacht – oder faktisch dauerhaft?
- [ ] **5. Systematische Überprufung externer Zugriffe**
  Werden externe Zugriffe systematisch überpruft und entzogen, sobald sie nicht mehr benötigt werden?

Kategorie: Daten & Compliance

- [ ] **6. Transparenz über sensible Daten**
  Wissen Sie konkret, wo Ihre sensiblen Daten liegen und wer aktuell Zugriff darauf hat?
- [ ] **7. Kontextabhängige Datenzugriffssteuerung**
  Wird der Zugriff auf sensible Daten kontextabhängig gesteuert – oder nur statisch erlaubt?
- [ ] **8. Nachweisbare Aufbewahrungsfristen**
  Können Sie jederzeit nachweisen, wie lange Daten gespeichert werden und warum?
- [ ] **9. Schnelle Datenbereitstellung**
  Sind Sie in der Lage, innerhalb von Stunden alle relevanten Daten fur einen Audit oder Incident bereitzustellen?

Mehr als 3x "Nein"?

Ihr Tenant hat signifikante Risiken. Wir helfen Ihnen, sie systematisch zu beheben.

www.cycura.de/termin